ANALISIS SISTEM *DIGITAL FORENSIC* PADA *VULNERABLE MACHINE* VULNOS2 BERDASARKAN *FRAMEWORK DIGITAL FORENSIC READINESS*

ANALYSING FORENSIC DIGITAL SYSTEM ON VULNERABLE MACHINE VULNOS2 BASED ON DIGITAL FORENSIC READINESS FRAMEWORK

Naufaldi Yusuf Hendriawan[1], Avon Budiyono[2], Adityas Widjajarto[3]

[1,2,3] S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]naufaldiyusuf@student.telkomuniversity.ac.id , [2]adtwjrt@telkomuniveristy.ac.id ,
[3]avonbudi@telkomuniversity.ac.id

Abstrak

Seiring dengan berjalannya waktu, tingkat kriminalitas yang ada di Indonesia pun juga semakin meningkat. Kriminalitas yang dilakukan juga ada banyak ragam, baik dengan cara tradisional ataupun dengan cara modern. Untuk cara modern, pelaku biasanya melakukan teknologi, teknologi yang paling sering pelaku gunakan biasanya merupakan komputer. Untuk mengatasi hal terbut, maka terdapat hal yang bernama forensik digital.

Pada penelitian ini dilakukan perhitungan risiko yang berdasar pada pendekatan *vulnerability* dan *threat*, setelah mendapatkan peringkat risiko dilakukan penentuan fungsi forensik berdasarkan peringkat risiko. Setelah mendapatkan fungsi forensik dilakukan pemilihan *software* yang dapat melakukan forensik pada VulnOS2 berdasarkan *framework Digital Forensic Readiness*. Data *vulnerability* didapatkan berdasarkan hasil *scanning* OpenVAS, sementara data *threat* didapatkan berdasarkan 10 *walkthrough* yang telah dipilih

Kata kunci : Forensik Digital, Peringkat Risiko, *Framework Digital Forensic Readiness* dan Fungsi Forensik.

Abstract

with how the time goes, criminality rate in indonesia has proven to be increasing as well. The criminality that has been done it have many variety as well, the traditional way or the modern way. For the modern way, the perpetrators usually using technology. Technology that the perpetrators mostly use is computer. To resolve it, then there is something called digital forensic.

In this research risk calculation is done based on vulnerability and threat approach, after getting risk ranking forensic function determination is done based on risk ranking. After getting forensic function choosing software that could do forensic on VulnOS2 based on Digital Forensic Readiness is done. Vulnerability data is obtained from OpenVAS scanning result, while threat data is obtained from 10 walkthrough that already chosen.

Keywords : Digital Forensic, Risk Ranking, Digital Forensic Readiness Framework and Forensic Function .

1. Pendahuluan

Pada era saat ini, teknologi merupakan salah satu hal paling penting untuk kehidupan sehari-hari. Untuk banyak orang, bahkan mereka tidak bisa memulai hari mereka tanpa melakukan sesuatu dengan teknologi mereka. Penggunaan teknologi itu sendiri juga termasuk kepada Indonesia. Dimana pengguna teknologi di Indonesia cukup banyak.

Banyak orang yang sangatlah memahami dalam penggunaan suatu teknologi. Penggunaan teknologi itu juga bermacam – macam, ada yang menggunakan teknologi tersebut untuk hal yang positif dan ada yang mengunakan teknologi tersebut untuk hal yang negatif. Orang yang menggunakan teknologi untuk hal yang negatif jumlahnya tidak sedikit, karena banyak yang melakukan hal tersebut.

*Tabel **Error! No text of specified style in document.**.1 Jumlah serangan* cyber *di tiap tahun*

No	Tahun	Jumlah serangan *cyber*
1	2014	11.000.000
2	2015	13.000.000
3	2016	15.000.000

Dari Tabel 1, dapat diketahui bahwa di indonesia terdapat 11 juta orang yang melakukan kriminalitas di tahun 2014, sementara terdapat kenaikan lagi untuk tahun tahun selanjutnya. Dan dapat diketahui lagi bahwa untuk peningkatan jumlah yang melakukannya relatif sama, yaitu dengan jumlah 2 juta orang yang melakukannya.

Dari hal tersebut, kita dapat mengetahui bahwa tingkat orang-orang yang menggunakan teknologi untuk melakukan kriminalitas cukup banyak, dan tiap tahunnya juga terdapat peningkatan jumlah yang termasuk ke kategori banyak. dan perlu diketahui lagi bahwa risiko tingkat kriminalitas melalui teknologi meningkat lagi juga sangat besar, karena semakin berjalannya waktu orang-orang menjadi semakin bergantung pada teknologi dan internet.

VulnOS2 adalah *Vulnerable Operating System* yang berjalan pada Ubuntu dan digunakan untuk melakukan pengecekan keamanan sistem. Akan tetapi pada VulnOS2 terdapat banyaknya celah keamanan yang dapat menyebabkan mudahnya sistem untuk diretas. Oleh karena itu, diperlukannya sistem yang dapat menangkap bukti kejadian saat terjadinya penyerangan pada sistem (*Digital Forensic*).

Digital forensic atau forensik digital salah satu cabang dari *forensic science* mencakup investigasi pada *material* yang ditemukan di perangkat digital [1]. Forensik digital biasanya dihubungkan dengan deteksi dan pencegahan kejahatan dunia maya. Forensik Digital berhubungan dengan keamanan digital yang berfokus pada kejadian digital [2].

Berdasarkan permasalahan yang didapatkan, dapat diketahui penelitian ini dilakukan untuk melakukan analisis fungsi forensik yang digunakan untuk memberikan rekomendasi *software Digital Forensic* yang cocok untuk VulnOS2. Pada penelitian ini akan menentukan fungsi forensik yang dimiliki VulnOS2 berdasarkan metode *Digital Forensic Readiness*.

2. Dasar Teori /Material dan Metodologi/perancangan

2.1. *Vulnerability*

Vulnerability atau kerentanan merupakan kelemahan pada keamanan yang dimiliki oleh sistem. Sebagai contoh pada prosedur, desain, atau implementasi, dapat dilakukan eksploitasi untuk menyebabkan kehilangan atau kerusakan. Sistem komputer juga mempunyai *vulnerability*. Sebagai contoh, sebuah sistem mungkin rentan terhadap data manipulasi yang tidak sah karena sistem tidak melakukan verifikasi identitas *user* sebelum mengizinkan akses data [3].

2.2 *Threat*

Threat atau ancaman merupakan sebuah keadaan yang mempunyai potensial untuk menyebabkan kehilangan atau kerusakan pada sistem komputer.terdapat banyak *threat* pada sistem konputer, termasuk dimulai dari manusia ataupundimulai dari komputer. Penyerangan juga bisa dimulai dari sistem lain [3].

2.3 *Digital forensic*

Forensik digital adalah sebuah forensik yang berhubungan dengan keamanan digital yang terfokus pada kejadian digital. Forensik digital mempunyai kesamaan teradap forensik komputer, akan tetapi forensik digital juga termasuk forensik dari semua teknologi digital. Investigasi tentang forensik digital dapat dibagi menjadi 3 bagian yaitu [2] :

1. Penjagaan bukti.
2. Analisis.
3. Presentasi/laporan.

Forensik digital menjadi pertanyaan yang tidak memiliki satu jawaban. Dalam praktiknya, ada lebih dari ratusan prosedur forensik digital yang dikembangkan di seluruh dunia. Namun prinsip dasarnya adalah sama: Pengintaian, Reliabilitas, dan Relevansi. Namun, sebuah framework bergantung pada partisipan dari organisasi tersebut [2].

Pada *Digital Forensic*, terdapat beberapa langkah yang harus dilakukan untuk mendapatkan suatu bukti digital, yaitu [4] :

1. Identifikasi bukti
2. Perolehan dan penjagaan bukti
3. Analisis bukti
4. Dokumentasi
5. Penyajian bukti

2.4 *Digital Forensic Readiness*

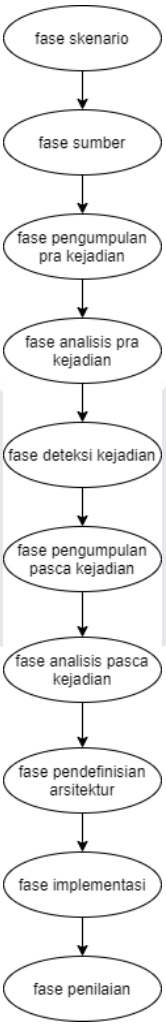
Digital Forensic Readiness (DFR) mempunyai 2 objektif. Objektif pertama adalah untuk memaksimalkan kemampuan sekeliling untuk mengumpulkan bukti digital yang konkret. Objektif kedua adalah untuk meminimalisir biaya untuk investigasi forensik saat tanggapan kejadian [5].

Para ahli mempunyai tanggapan yang berbeda-beda mengenai [5] :

1. Menurut Danielson dan Tjostheim mendefinisikan bahwa DFR berfokus pada mengadaptasikan organisasi dan mengkonfigurasi sistem mereka untuk aktif dalam mengumpulkan dan mempertahankan bukti untuk nantinya. Mereka melihat DFR meliputi persiapan umum untuk respon peristiwa, seperti menspesifikasikan bahan yang perlu dialokasikan pada tipe peristiwa yang berbeda. DFR dilihat sebagai sebuah bidang dalam sebuah bidang di forensic digital.
2. Rowlingson mendefinisikan bahwa DFR adalah kemampuan untuk memaksimalkan potensinya untuk menggunakan bukti digital dan juga meminimalisir biaya untuk investigasi. Rowlingson membuat perbedaan diantara aspek teknis dan organisasi dari DFR.
3. Hoolachan dan Glison mendefinisikan bahwa DFR adalah kemampuan dimana organisasi bisa mendahului kejadian kejahatan dengan mempersiapkan lingkungannya terlebih dahulu dan dengan melakukan hal ini, organisasi mendapatkan manfaat tidak hanya untuk instansi, tapi juga dalam membatasi risiko bisnis mereka.

2.5 *Framework Digital Forensic Readiness*

Framework Digital Forensic Readiness yang digunakan pada penelitian ini mengacu pada *paper* berjudul "*Towards a Digital Forensic Readiness Framework for Public Key Infrastructure Systems*" oleh Aleksander Valjarevic dan HS Venter. yang telah disesuaikan dengan studi kasus. Pada *framework* terdapat model yang digunakan, memiliki beberapa tahap yang digunakan. Berikut tahapan tahapan yang digunakan [1].

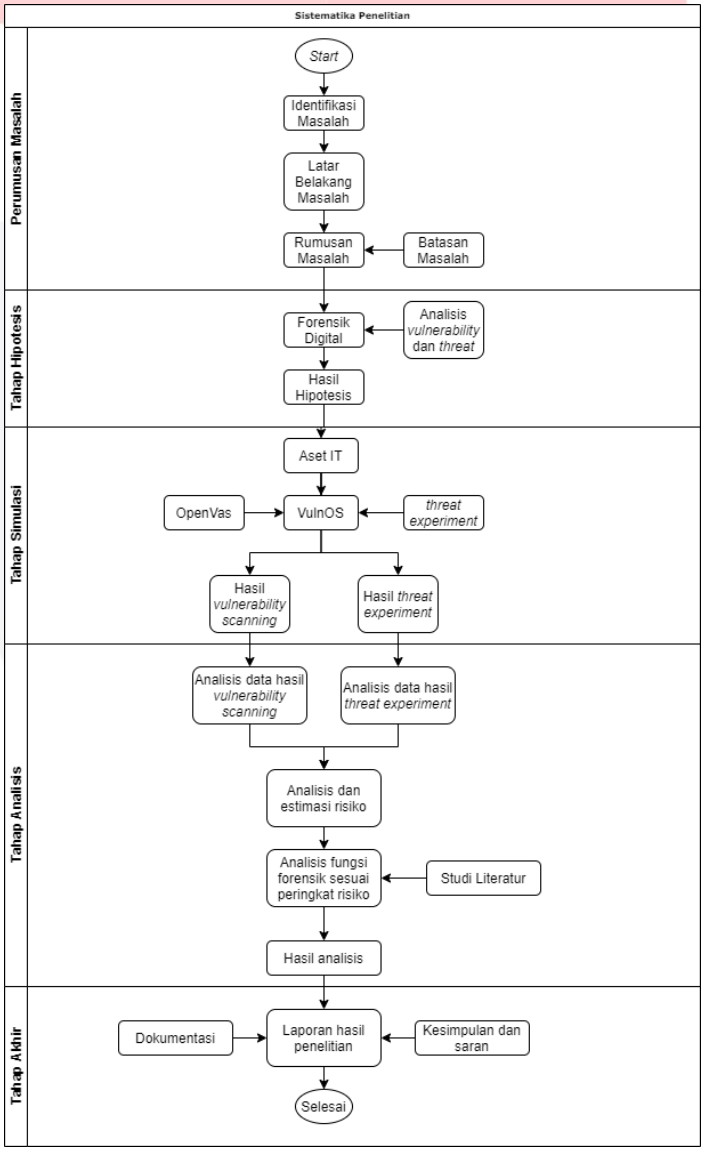


Gambar 1 langkah *framework Digital Forensic Readiness*

3. Metodologi

Metode yang digunakan untuk melakukan penelitian ini terbagi menjadi lima tahap yaitu perumusan masalah, tahap hipotesis, tahap simulasi, tahap analisis ,dan tahap akhir.

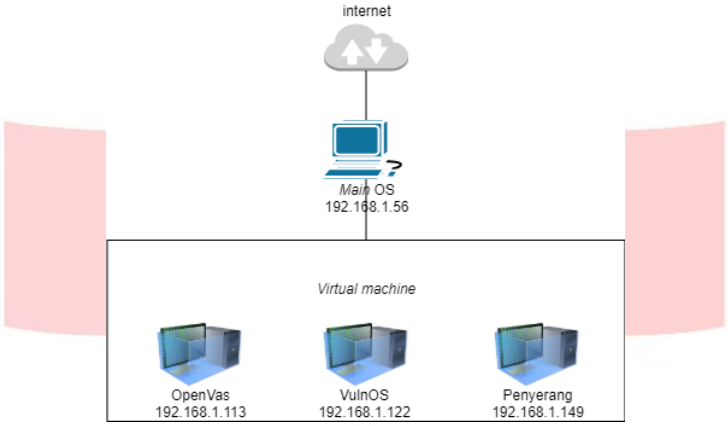
Pada tahap awal dimulai dengan melakukan identifikasi masalah terhadap latar belakang yang bertujuan untuk menggambarkan masalah yang akan diselesaikan pada penelitian ini. Kemudian didapatkan perumusan masalah dari penelitian ini yang dibatasi oleh Batasan masalah. Batasan masalah bertujuan untuk membuat penelitian menjadi lebih efektif, efisien dan tidak keluar dari topik penelitian ini. Pada tahap hipotesis dilakukan proses hipotesa bagaimana mendapatkan profil kebutuhan forensik berdasarkan risiko yang dihitung dari *vulnerability* dan *threat*. Dari perhitungan risiko tersebut akan didapatkan peringkat risiko. Pada tahap simulasi, dimulai dengan melakukan *scanning vulnerability* menggunakan OpenVas pada sistem *vulnerable* VulnOS. Dilakukan juga *threat experiment* berdasarkan *walkthrough*. Hasil yang didapatkan pada tahap simulasi adalah data *vulnerability* berupa hasil *vulnerability scanning* dan data *threat* berupa hasil *threat experiment*. Pada tahap analisis dilakukan analisis pada apa yang sudah didapatkan di tahap simulasi. Dilakukan analisis pada hasil *vulnerability scanning* dan hasil *threat experiment*. Dari hasil analisis, (berupa relasi eksploitasi dilanjutkan dengan estimasi risiko). (selanjutnya dilanjutkan dengan Analisa) peringkat risiko. Berdasarkan peringkat risiko dilakukan analisis fungsi forensik sesuai dengan peringkat risiko yang berdasarkan *framework Digital Forensic Readiness*. Pada tahap terakhir didapatkan hasil analisis sebagai kesimpulan. Pada tahap akhir hasil simulasi dan hasil analisis dapat dijadikan referensi laporan hasil penelitian. Dokumentasi dari penelitian yang dilakukan mendukung laporan hasil penelitian serta memberikan kesimpulan dan saran. *Output* akhir yang didapatkan adalah laporan dari hasil penelitian.



Gambar 2 Sistematika Penelitian

4. Perancangan Sistem

4.1 Topologi Fisik

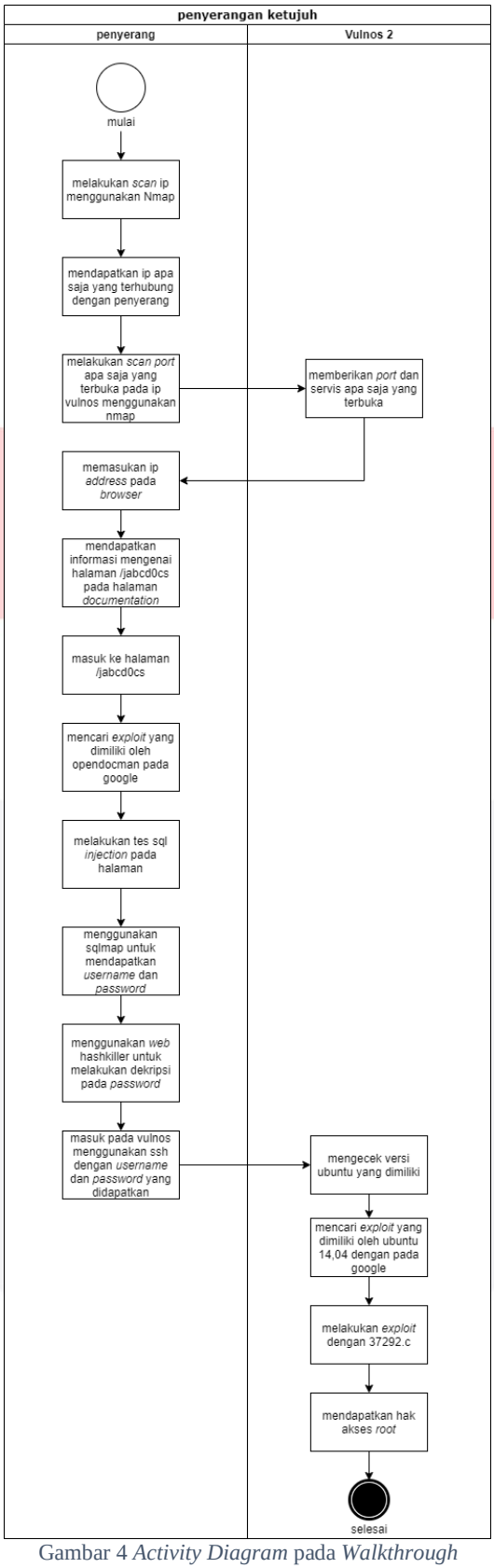


Gambar 3 Topologi Jaringan

Pada Gambar 3 terdapat topologi fisik yang digunakan pada penelitian ini. Terdapat *main* OS yang langsung terhubung dengan Internet. Setelah itu terhubunga pada VM (*Virtual Machine*) yang terdiri dari OpenVas, VulnOS dan penyerang.

Pada topologi fisik, Internet berfungsi sebagai penghubung terhadap koneksi untuk *virtual machine*. Dengan terdapatnya konseksi akan mempermudah pada pengalamatan, sehingga akan lebih mudah saat melakukan skenario pengujian *vulnerability scanning* dan skenario pengujian penyerangan. *Main* OS dan VM (*virtual machine*) berada pada satu jaringan. *Main* OS berfungsi sebagai penghubung antara internet dan *vulnerability machine* agar dimudahkan saat pengalamatan.

4.2 Perumusan *Activity Diagram*



Gambar 4 *Activity Diagram* pada *Walkthrough*

Pada Gambar 4 menjelaskan mengenai alur penyerang mendapatkan hak akses *root* dengan melakukan eksploitasi pada VulnOS2 yang dirancang dalam bentuk activity diagram. Pada Langkah pertama, dilakukan *scanning* IP menggunakan Nmap yang bertujuan untuk mendapatkan IP dari VulnOS, dengan cara melakukan *scanning* pada *network* IP *network* yang sama dengan penyerang. Selanjutnya melakukan *scanning port* pada IP menggunakan Nmap untuk mendapatkan *port* apa saja yang terbuka pada VulnOS2, dan mendapatkan *port* 22, 80 dan 6667 terbuka pada VulnOS2. Kemudian membuka IP pada *browser*. Setelah membuka IP pada browser dilakukan pengecekan pada halaman url dan didapatkan halaman baru pada halaman *Documentation* yaitu jabcd0cs. Setelah masuk pada halaman jabcd0cs ditemukan bahwa *website* menggunakan *OpenDocMan* dengan versi 1.2.7. setelah itu melakukan pencarian

eksploitasi pada *OpenDocMan* versi 1.2.7 dan mendapatkan *OpenDocMan* versi 1.2.7 lemah dengan SQL *injection*. Setelah mendapatkan kelemahan *OpenDocMan* 1.2.7 melakukan tes SQL *injection* pada halaman url. Setelah melakukan konfirmasi *OpenDocMan* 1.2.7 lemah terhadap SQL *injection* melakukan SQL *injection* menggunakan sqlmap pada OS untuk mendapatkan *username* dan *password* pada *database*. *Username* dan *password* akan digunakan untuk melakukan *login* pada OS. Selanjutnya setelah mendapatkan *username* dan *password* melakukan dekripsi pada enskripsi pada *password* di *web*. Setelah mendapatkan hasil dekripsi pada *password* melakukan *login* pada VulnOS menggunakan OpenSSH. Setelah melakukan *login* melakukan pengecekan versi Ubuntu. Setelah itu melakukan pengecekan eksploitasi yang dimiliki Ubuntu 14.04 pada *web* dan didapatkan Ubuntu 14.04 mempunyai kelemahan terhadap 37292.c. Selanjutnya Menggunakan wget untuk mengunduh *file* 37292.c. setelah mendapatkan *file* 37292.c melakukan *privilege escalation* hingga mendapatkan hak *super user*.

5. Pengujian Sistem dan Analisis

5.1 Analisis *Vulnerability* Berdasarkan *Scanning* OpenVAS

Berdasarkan analisis yang dilakukan, hasil *scanning* dengan CVSS 0.0 tidak termasuk pada kerentanan VulnOS2 karena tidak mempunyai pengaruh terhadap kerentanan sistem. Sesuai dengan analisis, *vulnerability* VulnOS 2 dipersingkat lagi dan pada masing masing *vulnerability* diberikan ID untuk melakukan penandaan pada *vulnerability*. pada *vulnerability* juga diberikan *threat level* sesuai dengan hasil pada *scanning* OpenVAS. Berikut *vulnerability* pada VulnOS2 sesuai dengan hasil analisis yang dilakukan.

Tabel **Error! No text of specified style in document.** VulnerabilityVulnOS2 dan rinciannya sesuai analisis

No	*Vulnerability*	*Service*	*Port*	CVSS	*Threat*
1.	Drupal *core critical remote code execution vulnerability*	HTTP	80	7.5	*High*
2.	SSH *weak encryption algorithm supported*	SSH	22	4.3	*Medium*
3.	SSH *weak* MAC *algorithm supported*	SSH	22	2.6	*Low*
4.	TCP *timestamps*	*General*	0	2.6	*Low*

5.2 Analisis Risiko Secara Kuantitatif Berdasarkan *Vulnerability* dan *Threat*

Tabel **Error! No text of specified style in document.**.2 Klasifikasi *Tools* Berdasarkan *Vulnerability* pada VulnOS

No	*Vulnerability*	CVSS	*Tools*	*Frequency*	*Risk*
1	Drupal Core Critical Remote Code Execution Vulnerability	7.5	Searchsploit	10	120
			Sqlmap	3	
			DIRB	2	
			Dirbuster	2	
2	SSH Weak Encryption Algorithms Supported	4.3	-	-	0
3	SSH Weak MAC Algorithms Supported	2.6	-	-	0
4	TCP timestamps	2.6	Netdiscover	1	28.6
			Nmap	10	

5.3 Analisis Fungsi Forensik Pada Sistem *Vulnerable* Berdasarkan Peringkat Risiko

Gambar 5 *Network Forensic*

Pada Gambar 5 terdapat hubungan antara *network forensic* dan *vulnerability* pada VulnOS2. Berdasarkan analisis dan studi literatur, didapatkan *vulnerability* "Drupal *core critical remote code execution vulnerability*" dan "TCP *timestamp*" berada pada *network forensic*. Karena hal tersebut, *software digital forensic* harus memiliki fitur untuk menangkap *network forensic*.

Gambar 6 *Computer Forensic*

Pada Gambar 6 terdapat hubungan antara *computer forensic* dan *vulnerability* pada VulnOS2. Berdasarkan analisis dan studi literatur, didapatkan *vulnerability* "SSH *weak encryption algorithm supported*" dan "SSH *weak* MAC *algorithm supported* berada pada *computer forensic*. Karena hal tersebut, *software digital forensic* boleh memiliki fitur untuk menangkap *computer forensic*, tapi tidak wajib.

5.4 Analisis *Software Digital Forensic* Yang Dibutuhkan VulnOS2 Berdasarkan *Framework Digital Forensic Readiness*

Tabel 3 Analisa software network forensic

No.	Nama *software*	Menangkap Apache *log*	Menangkap TCP *packet*
1.	Wireshark	✓	✓
2.	Tstat		✓
3.	Xplico	✓	✓
4.	Tcpdump		✓
5.	NetworkMiner	✓	✓

Pada Tabel 3 terdapat hasil Analisa yang telah dilakukan pada lima *software network forensic* pilihan. Didapatkan yang *support* untuk menangkap Apache *log* adalah Wireshark, Xplico dan NetworkMiner.

6. Kesimpulan

Setelah mendapatkan hasil analisis sistem *digital forensic* berdasarkan *framework Digital Forensic Readiness*, didapatkan beberapa kesimpulan. Analisis risiko didapatkan dari perhitungan *vulnerability* x *threat*, data *vulnerability* didapatkan dari *scanning* OpenVAS dan data *threat* didapatkan dari kumpulan *walkthrough*. Didapatkan risiko tertinggi ada pada *vulnerability* "Drupal *core critical remote code excecution vulnerability*" denan skor risiko 120. Peringkat risiko kedua dimiliki *vulnerability* "TCP *timetamps*" dengan skor risiko 28.6. peringkat ketiga dan keempat dimiliki *vulnerability* "SSH *weak encryption algorithm supported*" dan *vulnerability* "SSH *weak* MAC *algorithm supported*" dengan skor risiko yang sama yaitu 0. Berdasarkan peringkat risiko, didapatkan fitur yang harus dimiliki *software digital forensic* pada VulnOS2 adalah *network forensic*, sementara fitur *computer forensic* adalah fitur pelengkap. Berdasarkan Analisa yang dilakukan dengan *framework Digital Forensic Readiness* mendapatkan *software* Wireshark, Xplico dan NetworkMiner adalah *software digital forensic* yang dapat melakukan forensik pada VulnOS2.

7. Daftar Pustaka

[1] A. Valjarevic dan H. Venter, "Towards a Digital Forensic Readiness Framework for Public Key Infrastructure Systems," 2011.

[2] N. O. M. Sadiku, M. Tembely dan S. M. Musa, "Digital Forensics," *International Journal of Advanced Research in Computer Science and Software Engineering* , 2017.

[3] C. P. Pfleeger dan S. L. Pfleeger, Analyzing Computer Security: A Threat/vulnerability/countermeasure Approach, United States: Upper Saddle River, 2011.

[4] S. Raghavan, "Digital Forensic Research: Current State of The Art," 2012.

[5] M. A. Mankantshu, Investigating the Factors that Influence Digital Forensic Readiness in a South African Organisation, South Africa: University of Cape Town, 2014.